UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/693,749	10/24/2003	Thekkthalackal Varugis Kurien	MSFT-2839/301118.1	2449

41505 7590 09/27/2007

WOODCOCK WASHBURN LLP (MICROSOFT CORPORATION)
CIRA CENTRE, 12TH FLOOR
2929 ARCH STREET
PHILADELPHIA, PA 19104-2891

EXAMINER	
LE, CANH	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
09/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/693,749	KURIEN ET AL.	
	Examiner	Art Unit	
	Canh Le	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the application filed on 07/25/2007.

Claims 1-3, 13, 16-17, 20, 23, 25, 27-29, and 31 have been amended.

Claims 1-34 have been examined and are pending.

Double Patenting

The applicant file a terminal disclaimer on 725/2007 is acknowledged.

Response to Arguments

Applicant's arguments filed 07/25/2007 have been fully considered but they are not persuasive.

With regard to claim 1, The Applicant argues that:

England (Paul England, "A trusted Open Platform, IEEE Computer Society, July 2003, pp 55-62", hereinafter referred to as "England") "does not explicitly state or describe how data moves about the machine, possibly from the normal mode to Trusted mode, as present claim".

The Examiner respectfully disagrees:

In figure 2, England discloses machine monitor (e.g. virtual machine monitor). England discloses "Conceptually, machine partitioning accommodates these conflicting requirements by letting two or more operating systems run side by side on the same hardware, separated by a machine monitor [9]" [pg. 58, Col. 2]. A footnote 9 is listed on

page 62. According to Goldberg, the simulated machines are called virtual machines (Vs.), and the simulator software is called the virtual machine monitor (VMM) [page 35, col. 1]. The virtual machine supports multiple operating system execution concurrently with production uses of the system. It has capability to move data from one environment to another environment (See R. Goldberg, "Survey of Virtual Machine Research, " Computer, June 1974, pp.34-45). Therefore, the Examiner asserts that cited prior art does teach or suggest the subject matter recited in independent claim 1.

Regard claims 1 and 32, The Applicant argues that:

England does not discuss a single application being split functionally between two operating systems.

The Examiner respectfully disagrees:

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "a single application being split functionally between two operating systems") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

With regard to claim 8, The Applicant argues that:

"No disclosure is found for a machine monitor to incorporate such first identifier assign cryptographic mechanism".

The Examiner respectfully disagrees:

England teaches a code-based access (e.g. from machine monitor) which requires a method of establishing a program's identity. Sealed storage and attestation are two mechanisms that rely on code IDs [pg. 56, Col. 2 to pg. 57, Col. 1, "Definition of code ID ... For example, in the common"; fig. 1 & fig. 2; a code ID is equivalent to identifier. A base layer is equivalent to a machine monitor (e.g. virtual machine monitor)]]. England teaches the identity of a piece of code is its cryptographic digest, an operating system can measure and record an application program's code ID at the process creation [pg. 57]. Therefore, the Examiner asserts that cited prior art does teach or suggest the subject matter recited in dependent claim 8.

With regard claims 3, 4, 15, 17, and 29, The Applicant argues that:

"the Examiner's rejection fails in that no description, teaching or description of size or location of the potentially displayed encrypted text or graphics is shown or described in Willman, at all (US Patent Application No. 2005/0033980). Therefore there is no such teaching or suggestion to be possibly combined with England".

The Examiner respectfully disagrees:

Willman teaches the system of first software object causes a representation of said first of said plurality of data to be displayed on a display device, said representation comprising one or more indecipherable graphics **[par. [0012]; " secure output is similar. The information ... intercept it and read it"; an indecipherable graphics is**

equivalent to encrypted information. An encrypted information can be the same or different size].

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, It is proper to combine teaching of England and Willman.

With regard claims 21-22 and 27-28, The Applicant argues that:

"Claims 21-22, 27-28 depend either directly or indirectly upon allowable independent claims discussed and argued above regarding the 102 rejections, and are allowable for the same reasons. England does not teach each and every element of the rejected claim's respective independent base claim, not withstanding any possible addition of the teachings of Hayman (US Patent 5,895,966)".

The Examiner respectfully disagrees:

England teaches limitations in independent claims 1, 12, 25, and 32 as described above. Hayman teaches limitations in dependent claims 21-22 and 27-28.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by

combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, It is proper to combine teaching of England and Willman and further in view of Hayman because it would provide a security system controls who has access to a computer system and the extent of access to the system's resources n the system is accessed [Hayman, col. 1, lines 8-10].

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 26-31 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject mater.

Claims 26-31 are rejected under 35 U.S.C. 101 because it recites " a computer-readable medium having *encoded* thereon code". In the Specification, paragraph [0029], it recites "computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CDROM, digital versatile disks

(DVD) or other optical disk storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information and which can accessed by computer 110. Communication media typically embodies computer readable instructions, data structures, program modules or other data in a modulated data signal such as a carrier wave or other transport mechanism and includes any information delivery media. The term "modulated data signal" means a signal that has one or more of its characteristics set or changed in such a manner as to *encode information in the signal.* By way of example, and not limitation, communication media includes wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, RF, infrared and other wireless media. Combinations of any of the above should also be included within the scope of computer readable media". Encoding information in the signal is non-statutory. A computer-readable medium includes signal (see paragraph [0029) is non-statutory.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 8-14, 20, 23-26, and 32-34 are rejected under 35 U.S.C. 102(e) as being anticipated by **Paul England et al**. (hereinafter England, "A trusted Open Platform", IEEE Computer Society, July 2003, pp. 55-62).

As per claim 1, England teaches a system that manages the partitioning of an application comprising: a base layer that hosts the operation of a first environment and a second environment, the application comprising:

a first software object that executes in said first environment, said first software object handling a plurality of data and including logic to identify a first of said plurality of data as not processable by said first software object **[fig. 2, pg. 58, col. 2, "Figure 2 shows an NGSCB ... represents soft-"; pg. 59, par. [1]; application runs in normal mode (i.e. left half of figure). It would not process a data of trusted mode (i.e. right half of figure]**;

and a second software object that executes in said second environment and that processes said first of said plurality of data in a manner that resists tampering with said first of said plurality of data **[fig. 2, pg. 58, col. 2, "Figure 2 shows an NGSCB ... represents soft-"; pg. 59, col. 1, par. [1]; application runs in trusted mode (i.e. right half of figure)]**.

said base layer comprising or hosting logic that receives said first of said plurality of data from said software object and routes said first of said plurality of data to said second environment **[fig. 2, pg. 58, col. 2, "Figure 2 shows an NGSCB ... represents**

soft-"; pg. 59, col. 1, par. [1] & par. [2]; a machine monitor hosts applications running on normal mode and trusted mode].

As per claim 8, England teaches the system of claim 1, wherein said base layer comprises a component that assigns a first identifier to said second environment **[pg. 56, col. 2 to pg. 57, col. 1, "Definition of code ID ... For example, in the common"; fig. 1 & fig. 2; a code ID is equivalent to identifier. A base layer is equivalent to a machine monitor].**

As per claim 9, England teaches the system of claim 8, wherein said first of said plurality of data includes, or is accompanied by, said first identifier and a second identifier that identifies said second software object **[pg. 56, col. 2 to pg. 57, col. 1, "Definition of code ID ... For example, in the common"; fig. 1 & fig. 2; a code ID is equivalent to identifier. A base layer is equivalent to a machine monitor].**

As per claim 10, England teaches the system of first environment is associated with a first specification that describes the behavior of said first environment, wherein said second environment is associated with a second specification that describes the behavior of said second environment, wherein there is a higher level of assurance that said second environment will conform to said second specification than that said first environment will conform to said first specification **[fig. 2, pg. 58, col. 2, "Figure 2 shows an NGSCB...represent soft-"; pg. 59, col. 1, par. [1]; It is inherent that a**

first environment running on the LHS which relates to assurance is associated with specification that describe its behavior. A level of assurance of the trusted mode (i.e. RHS) is relatively higher than a level of assurance of the normal mode (i.e. LHS)].

As per claim 11, England teaches the system of claim 10, wherein said second software object relies upon the behavior of the second environment in order to resist tampering with said first of said plurality of data **[fig. 2; application runs on RHS].**

As per claim 12, England teaches the system of claim 1, wherein said base layer is said second environment, or is included within said second environment **[fig. 2, machine monitor].**

As per claim 13, England teaches a method of a first software object, which executes in a first environment, handling data to which an assurance policy applies, the method comprising:

the first software object encountering the data **[fig. 2, pg. 58, col. 2, "Figure 2 shows an NGSCB ... represents soft-"; pg. 59, par. [1]; application runs in normal mode (i.e. left half of figure). It's inherent that a first software object encountering a data]**;

the first software object determining that the data is not processable by the first software object **[fig. 2, pg. 58, col. 2, "Figure 2 shows an NGSCB ... represents soft-"; pg. 59, par. [1]; application runs in normal mode (i.e. left half of figure)]**;

the first software object causing the data to be provided to a second software object that executes in a second environment that provides a first level of assurance that actions performed in the second environment will be performed correctly, wherein the second software object processes the data in a manner that uses said assurance policy to create resistance to tampering with the data by acts arising outside of the second environment **[fig. 2; pg. 58, col. 2 to pg. 59, col. 1 , "NGSCB SYSTEM OVERVIEW... more hardware-based monotonic counters". Application runs on the left hand side (LHS) in normal mode. A right hand side (RHS) has Nexus and application or agent running on it. The nexus is a high-assurance OS kernel; a machine monitor monitors applications running on normal mode and trusted mode. It isolates a two systems to prevent them interfering with each other].**

As per claim 14, England teaches the method of claim 13, wherein the resistance to tampering comprises a resistance to a change in said data **[pg. 59, par. [2]; "The authenticated operation primitives enables each operating system ... from other operating system"; pg. 57, par. [4]; "seal uses an authentication encryption primitive to encrypt this data structure and to protect its integrity"; seal storage is another way to encrypt information].**

As per claim 20, England teaches the method of claim 13, wherein said policy specifies that said data is to be handled by said second software object **[pg. 59, col. 1, par. [1], "The right half of the figure ... from interfering with each other"; an application (i.e. second software object) runs on a high-assurance environment (i.e. RHS)]**

As per claim 23, England teaches the method of claim 13, wherein said second environment is associated with a first specification that describes the behavior of said second environment, and wherein said assurance policy provides that said second environment will conform to said specification **[fig. 2, pg. 59, col. 1, par. [1]; It is inherent that a second environment run on the RHS which relates to high-assurance is associated with specification that describe its behavior].**

As per claim 24, England teaches the method of claim 13, wherein said first environment is associated with a second specification that describes the behavior of said first environment, and wherein said first environment provides a second level of assurance that actions performed in the first environment will be performed correctly, said second level of assurance being relatively lower than said first level of assurance **[fig. 2, pg. 58, col. 2, "Figure 2 shows an NGSCB...represent soft-"; pg. 59, col. 1, par. [1]; It is inherent that a first environment run on the LHS which relates to assurance is associated with specification that describe its behavior. A level of assurance of the normal mode (i.e. LHS) is relatively lower than a level of assurance of the trusted mode (i.e. RHS)].**

As per claim 25, England teaches a computer-readable storage medium having encoded thereon code and data to allow a user to operate on first and second types of data, said second type of data requiring a relatively higher level of protection from tampering than said first type of data, said code and data comprising:

a first software object associated with a first specification that describes the behavior of said first software object, said first software object comprising instructions to:

operate on members of said first type of data **[fig. 2, application runs its data in a normal mode];**

recognize a member of said second type of data as not being processable by said first software object **[fig. 2, normal mode can not process data of trusted mode]**; and

cause said member of said second type of data to be routed to a second software object **[fig. 2, machine monitor routes data from normal mode to trusted mode]**; and

said second software object, which is associated with a second specification that describes the behavior of said second software object, there being a relatively higher level of assurance that said second software object will conform to said second specification than that said first software object will conform to said first specification, said second software object comprising instructions to operate on members of said

second type of data **[fig. 2; pg. 58, col. 2 , "Figure 2 shows an NGSCB ... represent soft-", pg. 59, col. 1, par. [1]]**.

As per claim 26, England teaches the computer-readable medium of claim 25, wherein said first software object operates in a first environment, wherein said second software object operates in a second environment, wherein said first environment is associated with a third specification that describes the behavior of said first software environment, wherein said second environment is associated with a fourth specification that describes the behavior of said second environment, wherein the level of assurance that said second environment will conform to said fourth specification is relatively higher than the level of assurance that said first environment will conform to said first specification, and wherein the assurance that said second software object will conform to said second specification derives from said second software object's reliance on the behavior of the second environment **[fig. 2; pg. 58, col. 2 , "Figure 2 shows an NGSCB ... represent soft-", pg. 59, col. 1, par. [1]]**.

As per claim 32, England teaches a system that supports the partitioning of an application into at least a first software object and a second software object, the system hosting a first environment and a second environment, the first software object running in the first environment, the second software object running in the second environment, the system comprising an application programming interface that exposes at least one of the following methods:

a first method that receives from the first software object a first data object that comprises: (1) data processable by the second software object, and (2) a first identifier assigned by the system to the second environment; and that routes said first data object to said second environment based on said first identifier **[fig. 2; pg. 58, col. 2, "Figure 2 shows an NGSCB ... represent soft-", pg. 59, col. 1, par. [1]; pg. 56, col. 2, "Definition of code ID ... have been used elsewhere"; a code ID is equivalent to a first identifier]** .

As per claim 33, England teaches the system of claim 32, wherein said first environment is associated with a first specification that describes the behavior of said first environment, wherein said second environment is associated with a second specification that describes the behavior of said second environment, wherein there is a first level of assurance that said first environment will conform to said first specification, wherein there is a second level of assurance that said second environment will conform to said second specification, and wherein said second level of assurance is relatively higher than said first level of assurance **[fig. 2, pg. 58, col. 2, "Figure 2 shows an NGSCB...represent soft-"; pg. 59, col. 1, par. [1]; It is inherent that a first specification that describes a behavior of a first environment running on the LHS (i.e. normal mode). A second specification describes a behavior of a second environment running on the RHS (i.e. trusted mode). A level of assurance of trusted mode is higher than a level of normal mode]**

As per claim 34, England teaches the system of claim 33, wherein said second software provides assurance that said second software object will protect data, said assurance being provided at least in part by relying on the behavior of the second environment **[fig. 2, pg. 59, par. [1]; applications run on a trusted mode (i.e. high-assurance)].**

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2-7, 15-19, 29, and 30-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over by **Paul England et al.** (hereinafter England, "A trusted Open Platform", IEEE Computer Society, July 2003, pp. 55-62), in view of **Willman et al.** (hereinafter Willman, US 2005/0033980 A1).

As per claim 2, England does not explicitly teach the system of first software object causes a representation of said first of said plurality of data to be displayed on a display device, said representation comprising one or more indecipherable graphics

Willman teaches the system of first software object causes a representation of said first of said plurality of data to be displayed on a display device, said representation

comprising one or more indecipherable graphics **[par. [0012]; " secure output is similar. The information ... intercept it and read it"; an indecipherable graphics is equivalent to encrypted information].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of England of the invention by including the step of Willman because it would provide secure input and output **[Willman, par. [0012]].**

As per claim 3, Willman further teaches the system of claim 2, wherein said one or more indecipherable graphics are either:

(1) the same size as each other **[par. [0012]; an encrypted information can be the same or different size]**, or

(2) of sizes that are unrelated to the content of said first of said plurality of data **[par. [0012]; an encrypted information can be the same or different size]**.

As per claim 4, England does not explicitly teach the system of the resistance to tampering provided by said second software object comprises said second environment resisting interference with the display of said first of said plurality of data by writing a representation of said first of said plurality of data into a video memory associated with a display device so as to cause said representation to supersede any image at a location on said display device at which said representation is to be displayed.

Willman teaches the system of the resistance to tampering provided by said second software object comprises said second environment resisting interference with the display of said first of said plurality of data by writing a representation of said first of said plurality of data into a video memory associated with a display device so as to cause said representation to supersede any image at a location on said display device at which said representation is to be displayed **[par. [0012]; NGSCB provides a secure output (i.e. RHS). "The information that appears onscreen can be presented ... intercept it and read it"].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of England of the invention by including the step of Willman because it would provide secure input and output **[Willman, par. [0012]].**

As per claim 5, England does not teach the system of first of said plurality of said is entered on a keyboard, and wherein the resistant to tampering provided by said second software object comprises resisting tampering with said first of said plurality of data in transit from said keyboard to an input stream of said second software object.

Willman teaches the system of first of said plurality of said is entered on a keyboard, and wherein the resistant to tampering provided by said second software object comprises resisting tampering with said first of said plurality of data in transit from said keyboard to an input stream of said second software object **[par. [0012], line 1-3;**

"keystrokes are encrypted before they can be read by software and decrypted once they reach the RHS"].

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of England of the invention by including the step of Willman because it would provide secure input and output **[Willman, par. [0012]].**

As per claim 6, England further teaches the system of claim 5, wherein said second application signs said first of said plurality of data to prevent subsequent tampering with said first of said plurality of data **[fig. 2, pg. 61, col. 1 "Document signing ... or certify the signing keys"].**

As per claim 7, England further teaches the system of claim 6, wherein said second environment signs said first of said plurality of data and the signature created by said second application as an indication that said first of said plurality of data and said signature were created in said second environment **[fig. 2, pg. 61, col. 1 "Document signing ... or certify the signing keys"]**.

As per claims 15, England does not explicitly teach a data is to be displayed on a visual display device, and wherein the resistance to tampering comprises displaying a representation of said data in a location on said visual display device and superseding any image other than said representation that is rendered at said location.

Willman teaches a data is to be displayed on a visual display device, and wherein the resistance to tampering comprises displaying a representation of said data in a location on said visual display device and superseding any image other than said representation that is rendered at said location **[par. [0012]; NGSCB provides a secure output (i.e. RHS). "The information that appears onscreen can be presented ... intercept it and read it"].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of England of the invention by including the step of Willman because it would provide secure input and output **[Willman, par. [0012]].**

As per claim 16, England does not explicitly teach a first software object causes a representation of the data to be displayed on a visual display device, said representation comprising one or more indecipherable graphics.

Willman teaches the method of claim 13, wherein said first software object causes a representation of the data to be displayed on a visual display device, said representation comprising one or more indecipherable graphics **[par. [0012]; " secure output is similar. The information ... intercept it and read it"; an indecipherable token is equivalent to encrypted information].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of England of the invention by

including the step of Willman because it would provide secure input and output **[Willman, par. [0012]].**

As per claim 17, Willman further teaches the method of claim 16, wherein said representation are either:

(1) the same size as each other **[par. [0012]; an encrypted information can be the same or different size],** or

(2) of sizes that are unrelated to the content of said data **[par. [0012]; an encrypted information can be the same or different size].**

As per claim 18, Willman further teaches the method of claim 16, wherein said first software object or said second software object, or a combination of said first software object and said second software object, cause items displayed on said visual display device to be changed in at least one respect to permit viewing of an image of the data produced by said second software object **[par. [0012]; "The information that appears onscreen ... no one else can intercept it and read it"; a secure out put is produced by application running on the RHS].**

As per claim 19, England does not explicitly teach a data is provided using a keyboard, and wherein the resistance to tampering comprises resisting a change to the data in transit from the keyboard to the input stream of the second software object.

Willman teaches a data is provided using a keyboard, and wherein the resistance to tampering comprises resisting a change to the data in transit from the keyboard to the input stream of the second software object **[par. [0012], line 1-3; "keystrokes are encrypted before they can be read by software and decrypted once they reach the RHS"].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of England of the invention by including the step of Willman because it would provide secure input and output **[Willman, par. [0012]].**

As per claim 29, England does not explicitly teach the computer-readable medium of first software object displays output on a visual display device, said output including one or more locations on said visual display device in which said member of said second type is to be displayed, and wherein said second software object displays a representation of said data of said second type in said one or more locations.

Willman teaches the computer-readable medium of claim 25, wherein said first software object displays output on a visual display device, said output including one or more locations on said visual display device in which said member of said second type is to be displayed, and wherein said second software object displays a representation of said data of said second type in said one or more locations **[par. [0012]; NGSCB provides a secure output (i.e. RHS). "The information that appears onscreen can be presented ... intercept it and read it"].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of England of the invention by including the step of Willman because it would provide secure input and output **[Willman, par. [0012]].**

As per claim 30, Willman further teaches the computer-readable medium of claim 29, wherein said representation is displayed in said one or more locations by said second environment causing said representation to be written into a video memory associated with said visual display device **[fig. 1, a video interface 190, a monitor 191; par. [0036], lines 23-26].**

As per claim 31, England does not teach the computer-readable medium of member of said second type comprises data to be entered using a keyboard, and wherein causing said member of said second type of data to be routed to said second software object comprises said second environment transporting said member of said second type from said keyboard to said second software object in a manner that resists tampering with said member of said second type by events arising outside of said second environment.

Willman teaches the computer-readable medium of member of said second type comprises data to be entered using a keyboard, and wherein causing said member of said second type of data to be routed to said second software object comprises said second environment transporting said member of said second type from said keyboard to said second software object in a manner that resists tampering with

said member of said second type by events arising outside of said second environment **[par. [0012], line 1-3; "keystrokes are encrypted before they can be read by software and decrypted once they reach the RHS"].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of England of the invention by including the step of Willman because it would provide secure input and output **[Willman, par. [0012]].**

Claims 21-22 and 27-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over by **Paul England et al.** (hereinafter England, "A trusted Open Platform", IEEE Computer Society, July 2003, pp. 55-62), in view of **Hayman et al.** (hereinafter Hayman, US patent 5,895,966).

As per claim 21, England does not explicitly teach data includes, or is associated with, a first label that identifies said second environment as a location in which said data is to be processed.

Hayman teaches data includes, or is associated with, a first label that identifies said second environment as a location in which said data is to be processed **[abstract, fig. 3A, fig. 3B, col. 1, lines 63-64, col. 5, line 24 to col. 6, line 36; security labels are placed on each data file].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of England of the invention by

including the step of Hayman because it would provide a security system controls who has access to a computer system and the extent of access to the system's resources on the system is accessed **[Hayman, col. 1, lines 8-10].**

As per claim 22, Hayman further teaches the method of claim 21, wherein said data includes, or is associated with, a second label that identifies said second software object as a processor for said data, and wherein said second environment routes said data to said second software object based on said second label **[abstract, fig. 3A, fig. 3B, col. 1, lines 63-64, col. 5, line 24 to col. 6, line 36].**

As per claim 27, England does not explicitly teach the computer-readable medium of each member of said second type of data comprises: (1) a first label indicating that said member of said second type is to be processed in said second environment, and (2) a second label assigned by said second environment indicating that said member of said second type is to be processed by said second software object.

Hayman teaches the computer-readable medium of each member of said second type of data comprises: (1) a first label indicating that said member of said second type is to be processed in said second environment, and (2) a second label assigned by said second environment indicating that said member of said second type is to be processed by said second software object **[abstract, fig. 3A, fig. 3B, col. 1, lines 63-64, col. 5, line 24 to col. 6, line 36].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of England of the invention by including the step of Hayman because it would provide a security system controls who has access to a computer system and the extent of access to the system's resources on the system is accessed **[Hayman, col. 1, lines 8-10].**

As per claim 28, Hayman further teaches the computer-readable medium of claim 27, wherein said first software object causes said member of the second type to be routed to said second software object by sending said member of the second type to a base component, said first label being assigned by said base component, said second label being recognizable by said second environment and not by said base component **[abstract, fig. 3A, fig. 3B, col. 1, lines 63-64, col. 5, line 24 to col. 6, line 36]**.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Canh Le

September 22, 2007

SYED A. ZIA
PRIMARY EXAMINER